

REMARKS

Applicant has not amended original Claims 1 through 37. Applicant has added a new Claim 38 directly to a self contained stand alone security device in accordance with the present invention as described in the specification which includes the function of repeatedly verifying the identity of the user during the period of admission.

The rejection of Claims 1-37 under 35 U.S.C. §102(b) as allegedly being anticipated by Fischer (EPA EP 0770 953 A2) (hereinafter "Fischer") is hereby traversed.

For a prior art reference to anticipate in terms of 35 U.S.C. §102, every element of the claimed invention must be identically shown in a single reference. In re Bond, 15 USPQ2d 1566, 1567 (Fed. Cir. 1990). These elements must be arranged as in the claim under review. Id.

The Fischer reference does not disclose the same invention as set forth in Claims 1, 22 and newly added Claim 38. Fischer discloses a smart card or similar device which utilizes at least one clock and preferably two trusted clocks which generate an average precise time and a random value generator 10 in the smart card which is used by processor 4 in the digital signature process. See column 4, lines 34-40. Applicant's security device does not utilize a random number generator in the security device. In Applicant's invention, the host utilizes a random number generator to generate a random value.

The method and apparatus of Applicant's claimed invention requires the sending of a message by the security device associated with the person whose identity is to be verified, the message including the person's public key number. This public key number message is

Amend03.315
909-1

-9-

received by the host. The host encrypts a random message using the public key number and sends the public key number encrypted random message to security device. The security device decrypts the public key number encrypted random message using the person's private key number and sends the decrypted random message to the host. The host compares the decrypted random message sent by the security device with the random message previously encrypted by the host with the public key number to verify the identity of the person. These steps may be repeated during the period of admission or processing without involvement of the identified person. Such a system is not disclosed by Fischer.

For example, the Examiner cites column 7, lines 10-22 and line 26-33 for the element of the first clause of Claim 1, i.e. sending a message by said security device associated with the person whose identity is to be verified, said message including said person's public key number. The cited language of column 7 of Fischer does not support a disclosure of the claim element. Fischer in the cited location includes certification authority insuring that the public key numbers match with the private key number by means of a certificate issued by the device manufacturer associating the public key with the trusted device. Fischer also goes on to state that the user's certifier vouches that the trusted device contains the user's private key and also provides trusted times so that only the single certificate is required. The security device of Fischer is sending a certificate of the manufacturer, it is not sending a public key number of the person to be identified. The language at lines 26-33 of column 7 go on to talk about that there are some additional steps required by the certifier or the user beyond those that may normally be taken to simply confirm the public key is associated with the user. The additional steps confirm that the user's public key is indeed also associated

Amend03.315
909-1

-10-

with a trusted date/time notary device. Again, there is no disclosure of the security device sending the public key number of the person to be identified to a host. The security device in Fischer is sending a certificate of the manufacturer.

Further, there is no support in Fischer for the second element as recited in the second clause of Claim 1, namely "receiving said message by a host, said host encrypting a random message using said public key number and sending said public key number encrypted message to said security device." The examiner cites column 7, lines 26-45 of Fischer. Again, the cited portion talks about some additional steps being required by the certifier or user beyond those that may normally be taken to simply confirm that the public key is associated with the user. Again, the reference is made to the fact that additional steps confirm that the user's public key is indeed also associated with the trusted date/time notary device. Fischer goes on to state that in order to certify the user, initially a validation step is performed in which a validating certificate provided by the manufacturing device indicates that the subject public key is properly associated with the notary device in question. Fischer goes on to state that the user's public key is properly associated with the notary device may be confirmed by issuing a challenge with the expectation of getting a predetermined response to confirm that the subject key properly associated with the notary device. Fischer further goes on to state that the notary device may be operated in the certifier's presence against random challenge data supplied by the certifier so that the certifier is assured that the actual device produces an expected signature (as verified with the anticipated public key). This language is not an enabling disclosure of a public key number message being received by the host, the host encrypting a random message using the public key number and sending the

Amend03.315
909-1

-11-

public key number encrypted message back to the security device.

The next step in Claim 1 is "said security device decrypting said public key number encrypted random message using said person's private key number and sending said decrypted random message to the host." The Examiner cites column 6, lines 56 through column 7, line 10. It is noted that the cited portion of the text is prior to the text previously disclosed. Fischer does not operate in the same manner as Applicant's disclosure. The Examiner is selecting language in the Fischer reference to meet language in the claims, but the elements and function are not in the same order and are not arranged in the same manner in Fischer and in the claimed invention. Accordingly, Fischer is not a 35 U.S.C. §102 reference. Further, the Examiner cites column 6, line 56 through column 7, line 10. The cited language of Fischer talks about the notary device of Figure 1 being designed to be implemented in accordance with various alternate embodiments or modes of invention. A first mode of operation using a single private key. In this mode there is a single resulting digital signature and a single certificate. Fischer goes on to state that the certificate establishes that a particular user is operating with the private key and a trusted notary device. Fischer goes on to state that in this implementation, the certifier explicitly indicates in the user's certificate that the user's private key is embodied in a device with a trusted clock. Fischer goes on to state that this may also be accomplished indirectly if the certifier was known (either explicitly or implicitly) to only certify users whose private key is operated with secured devices with trusted clocks. The quoted language at the bottom of column 6 and the top of column 7 of Fischer does not support the third clause of Claim 1 of the security device decrypting the public key number encrypted random message using the

person's private key number and sending the decrypted random message back to the host.

The quoted language talks about a certificate of the manufacturer or that the manufacturer is known to certify only users whose private key is operated within a secure device with trusted clocks.

The last clause of Claim 1 requires that the host compare the decrypted random message sent by the security device with the random message previously encrypted by the host with said public key number to verify the identity of the person. The Examiner cites column 7, lines 41-55. Again, there is no disclosure of this subject matter in the cited lines. The specific element set forth in Claim 1 are not set forth in Fischer. Fischer merely talks about, "initially a validation step is performed in which a validating certificate provided by the manufacturing device indicates that the subject public key is properly associated with the notary device in question." Fischer goes on to state that, "the user's public key is properly associated with the notary device may be confirmed by issuing a challenge with the expectation of getting a predetermined response to confirm that the subject key is properly associated with the notary device." This is not an adequate disclosure of Applicant's claimed invention and in fact Fischer does not disclose Applicant's claimed invention.

The steps and apparatus disclosed and claimed by Applicant in Claims 1, 22 and 38 are not disclosed by Fischer.

Fischer does not disclose the structure of the apparatus defined by Claim 22 as required by 35 U.S.C. §102. Fischer is not an anticipatory reference with respect to Claim 22.

The first clause of Claim 22 recites "means for permanently storing a corresponding

private key number and a public key number assigned to said person." The Examiner's attention is directed to Figure 1 and the abstract which clearly shows and states that box 6 of Fischer is a "secret private key storage." There is no disclosure in Fischer of a smart card having a means for permanently storing a corresponding private key number and a public key number assigned to said person. This is not only a substantial difference in structure, but it also shows that the two systems operate completely differently. The smart card of Fischer utilizes a random value generator 10 to generate a digital signature. Certificates of the manufacturer are supplied by the smart card of Fischer for identification.

The second clause of Applicant's Claim 22 recites "means for sending said public key number to a host seeking to verify the identity of said person." The Examiner cited column 7, lines 10-22 and lines 26-33. There is no specific disclosure in Fischer of a means for sending the public key number to a host seeking to verify the identity of the person. In Fischer, a certificate issued by the device manufacturer is utilized.

The third clause of Claim 22 requires "means for receiving from said host a random message encrypted with said public key number." The Examiner cites column 7, lines 26-45. There is no disclosure in Fischer of means for receiving from the host a random message encrypted with the public key number. Fischer only talks about a challenge with expectation of getting a predetermined response to confirm that the subject key is properly associated with the notary device. Fischer goes on to state that the actual device produces an expected signature, which as described above, is produced by a random generator 10 input into processor 4 of the Fischer smart card. Fischer goes on the state that the certifier also checks that the date/time produced by the device is correct. Fischer is relying heavily on the

date/time element in its verification process, which is not a part of Applicant's claimed invention.

The fourth clause of Claim 22 requires "means for decrypting said random message encrypted with said public key number." The Examiner cited column 6, line 56 to column 7, line 10. Again, this is not disclosed in Fischer.

The fifth clause of Claim 22 requires "means for sending said decrypted random message to said host for comparison to said random message previously encrypted with said public key number to verify the identity of said person." The Examiner cites column 7, lines 41-55. Again, this structure is not disclosed in Fischer.

Although Fischer and Applicant talk about things such as public and private keys, encryption and decryption, and random messages, the elements in Fischer are not put together as set forth in Applicant's claim for a simple system for identifying and continually verifying and identifying the identity of a user. The Fischer reference is directed to producing a validated signature which can be validated both at the time of execution of the signature and at some time and any time in the future as long as the signature was properly valid at the time that it was made. That is, in Fischer, the signature remains valid as a result of its time stamp even though the user's public key number may become inactive or invalid at some time after the signature was made. Applicant's invention and the disclosure of Fischer are directed to two different things. Fischer is not a complete disclosure of Applicant's claimed invention as required by 35 U.S.C. §102.

As set forth above, newly added Claim 38 adds additional elements to the subject matter of Claim 22. Accordingly, Claim 38 also patentably distinguishes over the Fischer

reference.

Claims 2-21 add additional subject matter to the method of Claim 1 and clearly by definition patentably distinguish over the Fischer reference.

Claims 23-37 add additional subject matter to Claim 22 and by definition clearly patentably distinguish over the Fischer reference.

The purported addition of U.S. Pat. No. 6,779,024 - DeLaHuerga ("DeLaHuerga") to the Fischer reference does not anticipate nor make obvious Applicant's claimed invention as set forth in Claims 1, 22 and 38. There is no suggestion in either of these references of a motivation to combine the two references. The mere fact that they are both in the computer field is not a sufficient motivation to combine them. Everything in the field of computers is not automatically combinable, otherwise nothing would be patentable. Since the independent Claims 1, 22 and 38 patentably distinguish over the combination of Fischer and DeLaHuerga, the dependent claims, by definition, must also patentably distinguish over the purported combination of these two references.

In view of the above, it is respectfully submitted that this application with Claims 1-38 is allowable over the art of record. An early office action toward that end is earnestly solicited.

If an extension of time is necessary for this Response to be timely filed, Applicant hereby requests an extension of time to make this Response timely filed.


Authorization is hereby given to charge to undersigned's deposit account no. 16-1428 all required fees in connection with the request for extension of time or in connection with any other fees that may be due as a result of the filing of this Response. You are hereby

Amend03.315
909-1

-16-


authorized to charge the correct amount of the fee and/or to credit any overpayment to the undersigned's deposit account no. 16-1428. A claim for small entity status has been previously filed in this application.

Respectfully Submitted,


MICHAEL F. PETOCK, ESQUIRE
Registration No. 26,015
46 The Commons at Valley Forge
1220 Valley Forge Road
P.O. Box 856
Valley Forge, PA 19482-0856
Telephone (610) 935-8600
Facsimile (610) 933-9300
Attorney for Applicants

Certificate of Facsimile

I hereby certify that this correspondence is being facsimile transmitted to facsimile no. (703) 872-9306 at the United States Patent and Trademark Office on the date shown below.


MICHAEL F. PETOCK, ESQ.

4/12/05
DATE